POSTAL SE

Privacy Act of 1974; System of Records

AGENCY: U.S. Postal Service®.

ACTION: Notice of a modified system of records.

SUMMARY: The United States Postal Service® (USPS®) is proposing to revise a Customer Privacy Act Systems of Records (SOR). These modifications are being made to reflect enhanced functionality within an integrated technology system that supports USPS Identity Verification Services (IVS) and will seek to enhance In-Person Identity Proofing Capabilities to voluntarily align with National Institute of Standards and Technology (NIST) 800.63A Digital Identity standards. This enhanced functionality will be used to meet internal USPS needs and the requirements of other Federal government agencies. Modifications to this SOR are also being proposed to support a separate initiative that enhances the In-Person enrollment process for the Informed Delivery® feature, with an objective to improve the customer experience.

DATES: These revisions will become effective without further notice on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, unless, in response to comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be submitted via email to the Privacy and Records Management Office, United States Postal Service Headquarters (privacy@usps.gov). To facilitate public inspection, arrangements to view copies of any written comments received will be made upon request.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or privacy@usps.gov.

SUPPLEMENTARY INFORMATION: This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the Federal Register when there is a revision, change, or addition, or when the agency establishes a new system of records. The Postal Service has determined that Customer Privacy Act System of Records USPS 910.000 Identity and Document Verification Services, should be revised to support efforts to enhance

identity proofing capabilities and voluntarily align with new digital identity standards set forth by NIST. Additional proposed modifications support enhancements to the In-Person enrollment process for the Informed Delivery feature.

I. Background

The Postal Service utilizes a modern integrated Identity Verification System (IVS) to optimize, manage, and develop the Postal Service capabilities to support Identity Proofing for USPS, and other Federal Agencies under agreement with USPS, to provide identity verification services. Services provided by USPS may include biometric fingerprint collection, remote proofing, In-Person proofing webservices and Application Programming Interfaces (APIs) that enable the support and fulfillment of Federal agency requirements. USPS SOR 910.000, Identity and Document Verification, is being modified to reflect enhanced functionality within this integrated Identity Verification Services (IVS) system.

The Postal Service is seeking to enhance USPS's identity proofing capabilities. The objectives of this initiative will advance the mission of the Postal Service by:

- Providing additional Identity proofing capabilities to meet requirements set forth in agreements with participating Federal Agencies, as authorized by 39 U.S.C. 411
- Improve the effectiveness and security of USPS internal identity proofing capabilities and processes

The Postal Service is voluntarily aligning its capabilities and processes with selected guidelines and standards for In-Person identity proofing from the National Institute of Standards and Technology (NIST). USPS offers an In-Person Proofing (IPP) service to support individuals that are not able to verify their identity remotely online. In-Person proofing capabilities provide different levels of certainty for which a user's identity claim can be assessed at an accepted level of trust to determine eligibility for access to applications and uses. By enhancing identity proofing capabilities and processes, the Postal Service is positioning itself to better support the needs of other Federal Agencies that require identity proofing services. The Postal Service is uniquely positioned to offer In-Person proofing services at selected Retail Post Offices, across its large Retail Network, with the added values of accessibility and convenience.

Currently, the IPP Basic capability is used to support the Informed Delivery feature at USPS. However, the IPP program continues to mature to support potential Federal use cases or requirements, and advanced capabilities. The future vision and roadmap for the USPS IPP program will include the ability to support advanced identity proofing standards for sensitive or risk averse transactions that would require real-world evidence to ensure that the user is who they claim to be. The new and enhanced In Person proofing capability will voluntarily align with NIST 800.63A guidelines for Identity Proofing at the Identity Assurance Level (IAL), Level 2 (IAL-2). In this context, the Identity Proofing process utilizes attribute information provided by the individual applicant, such as name, address of residence, phone number and email address, that is subsequently validated using various forms of identity evidence and documentation. The goal of identity verification is to confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the evidence, thereby ensuring that the individual user is who they claim to be and minimizing the risk of fraud or misuse.

More detailed information that pertains to Identity Proofing Requirements may be obtained from NIST Special Publication 800-63, Digital Identity Guidelines available for viewing at https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines. As described by NIST, “The Special Publication (SP) 800-63 document suite provides technical requirements for federal agencies implementing digital identity services in a four-volume set: SP 800-63-3 Digital Identity Guidelines, SP 800-63A Enrollment and Identity Proofing, SP 800-63B Authentication and Lifecycle Management, and SP 800-63C Federation and Assertions. The publication provides security and privacy controls for digital identity management for designated levels of assurance, including identity proofing, authentication and use of authenticators, and identity federation. SP 800-63-3 establishes risk-based processes for the assessment of risks for identity management activities and selection of appropriate assurance levels and controls. Organizations have the flexibility to choose the appropriate assurance level to meet their specific needs.”

As indicated above, by voluntarily aligning with the NIST Digital Identity Guidelines for Enrollment and Identity Proofing as outlined in NIST SP-800.63A, the Postal Service can attain certification at the IAL-2 Level, that will enhance the ability to meet the future needs of other Federal Agencies as authorized by 39 U.S.C. 411, via interagency agreements. Obtaining IAL-2 Level certification will enhance In-Person Proofing capabilities available through the Postal Service and the ability to support other Federal Agency initiatives and partnerships that require IAL-2 level Identity Proofing services.

The Postal Service is also proposing to enhance the In-Person enrollment process for the Informed Delivery feature by streamlining the process steps and combining aspects for determining eligibility and identity proofing. The customer will have the option to voluntarily have the barcode on the back of their government issued IDs scanned to capture name and address information that will be used to confirm eligibility for the Informed Delivery feature, and to prefill that information during the enrollment process. The objective of this Informed Delivery initiative is to improve efficiency by combining similar information collected across the In-Person enrollment process when customers sign-up for the Informed Delivery feature.

II. Rationale for Changes to USPS Privacy Act Systems of Records

The Postal Service is proposing to modify USPS SOR 910.000 in support of enhancing In-Person Proofing, Identity Proofing Capabilities to support both USPS and external Federal Agencies by voluntarily aligning with NIST 800.63 standards.

The Postal Service requires the need to capture and store a customer or participants name, address, phone number, personal email, high-resolution images and associated attribute information, then validate the information collected using various forms of identity evidence and documentation to enhance Identity Proofing capabilities that will be used to:

- Verify the authenticity of the person’s associated Identity Documents to further confirm their proof of Identity
- Align with audit requirements for storing and maintaining Personally Identifiable Information (PII)
- Voluntarily align with NIST 800.63 Identity Verification guidelines and standards

- Provide USPS with the ability to provide Identity Proofing services to other partnering Federal Agencies
- Provide reporting capabilities for USPS and other partnering Federal Agencies
- Provide the Postal Service with the ability to be certified at the 800.63A IAL-2 level, increasing the USPS security posture and the ability to meet the security requirements of other Federal Agency partnerships.

Accordingly, to support enhanced In-Person Proofing, Identity Proofing capabilities, three new purposes are being added to USPS SOR 910.000, along with proposed modifications to three existing purposes. A new Category of Records and record retention and disposal policy that pertain to records maintained for Identity Proofing activities are also being added to support the enhanced IPP initiative.

In addition, the Postal Service is proposing to modify SOR 910.000, to include two new purposes in support of enhancements to the In-Person enrollment process for the Informed Delivery feature. Similarly, modifications to USPS SOR 820.300, Informed Delivery are being proposed and will be described in a separate Federal Register Notice.

III. Description of the Modified System of Records

Pursuant to 5 U.S.C. 552a(e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed revisions to this SOR has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect this modified system of records to have any adverse effect on individual privacy rights. Accordingly, for the reasons stated above, the Postal Service proposes revisions to this system of records. SOR 910.000 Identity and Document Verification is provided below in its entirety.

SYSTEM NAME AND NUMBER:

USPS 910.000, Identity and Document Verification Services.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

USPS Marketing, Headquarters; Integrated Business Solutions Services Centers; and contractor sites.

SYSTEM MANAGER(S):

Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1500.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, 404, and 411.

PURPOSE(S) OF THE SYSTEM:

1. To provide services related to identity and document verification services.

2. To issue and manage public key certificates, user registration, email addresses, and/or electronic postmarks.

3. To provide secure mailing services.

4. To protect business and personal communications.

5. To enhance personal identity and privacy protections.

6. To improve the customer experience and facilitate the provision of accurate and reliable delivery information.

7. To identify, prevent, or mitigate the effects of fraudulent transactions.

8. To support other Federal Government Agencies by providing authorized services.

9. To ensure the quality and integrity of records.

10. To enhance the customer experience by improving the security of Change-of-Address (COA) and Hold Mail processes, along with other products, services and features that require identity proofing and document verification.

11. To protect USPS customers from becoming potential victims of mail fraud and identity theft.

12. To identify and mitigate potential fraud in the COA and Hold Mail processes, along with other products, services and features that require identity proofing and document verification.

13. To verify a customer's identity when applying for COA and Hold Mail services, along with other products, services and features that require identity proofing and document verification.

14. To provide an audit trail for COA and Hold Mail requests (linked to the identity of the submitter).

15. To enhance remote identity proofing with a Phone Verification and One-Time Passcode solution.

16. To enhance remote identity proofing, improve fraud detection and customer's ability to complete identity proofing online with a Device Reputation Remote Identity Verification solution.

17. To verify a customer’s Identity using methods and Identity Proofing standards that voluntarily align with NIST Special Publication 800.63 and support other Federal Agency partner security requirements.

18. To enhance In-Person identity proofing, improve Identity Document fraud detection and enable a customer to successfully complete identity proofing activities required for access to Postal Service products, services and features.

19. To enhance In-Person identity proofing, improve Identity Document fraud detection and enable a customer to successfully complete identity proofing activities as required by partnering Federal Agencies to authorize or allow individual customer access to a privilege, system, or role.

20. To facilitate the In-Person enrollment process for the Informed Delivery® feature.

21. To provide customers with the option to voluntarily scan the barcode on the back of government issued IDs to capture name and address information that will be used to confirm eligibility and prefill information collected during the In-Person Informed Delivery enrollment process.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Customers who apply for identity and document verification services.

2. Customers who may require identity verification for Postal products, services and features.

3. USPS customers who sign-up, register or enroll to participate as users in programs, request features, or obtain products and/or services that require document or identity verification.

4. Individual applicants and users that require identity verification or document verification services furnished by the Postal Service in cooperation with other Government agencies.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Customer information: Name, address, customer ID(s), telephone number, text message number and carrier, mail and email address, date of birth, place of birth, company name, title, role, and employment status.

2. Customer preference information: Preferred means of contact.

3. Authorized User Information: Names and contact information of users who are authorized to have access to data.

4. Verification and payment information: Credit or debit card information or other account number, government issued ID type and number, verification question and answer, and payment confirmation code. (Note: Social Security Number and credit or debit card information may be collected, but not stored, in order to verify ID.)

5. Biometric information: Fingerprint, photograph, height, weight, and iris scans. (Note: Information may be collected, secured, and returned to customer or third parties at the request of the customer, but not stored.)

6. Digital certificate information: Customer's public key(s), certificate serial numbers, distinguished name, effective dates of authorized certificates, certificate algorithm, date of revocation or expiration of certificate, and USPS-authorized digital signature.

7. Online user information: Device identification, device reputation risk and confidence scores.

8. Transaction information: Clerk signature; transaction type, date and time, location, source of transaction; product use and inquiries; Change of Address (COA) and Hold Mail transactional data.

9. Electronic information: Information related to encrypted or hashed documents.

10. Recipient information: Electronic signature ID, electronic signature image, electronic signature expiration date, and timestamp.

11. In-Person Proofing and Enhanced Identity Verification Attributes: Contents of Valid Identification (ID) Documents; High resolution images of front and back of ID documents, bar

code on ID Document and the content of displayed and encoded fields on ID documents that may be collected and stored in order to facilitate security validation and Identity Proofing of an applicant, participant or customer's ID; Facial Image; Name, Address, and Unique ID Document number; Birthdate, Eye Color, Height and Weight; Signature; Organ donation preference.

12. Strong ID Documents used for In-Person Identity Proofing: Photo ID, unique ID Number and the name of the Individual being identified; Passports, Passport cards; State ID Cards, State Driver's Licenses: Uniformed Service ID's, and Government ID documents.

RECORD SOURCE CATEGORIES:

Individual Customers, Users, Participants and Applicants

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Standard routine uses 1. through 7., 10., and 11. apply.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated databases, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

By customer name, customer ID(s), distinguished name, certificate serial number, receipt number, transaction date, and email addresses.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Records related to Pending Public Key Certificate Application Files are added as received to an electronic database, moved to the authorized certificate file when they are updated with the required data, and records not updated within 90 days from the date of receipt are destroyed.

2. Records related to the Public Key Certificate Directory are retained in an electronic database, are consistently updated, and records are destroyed as they are superseded or deleted.

3. Records related to the Authorized Public Key Certificate Master File are retained in an electronic database for the life of the authorized certificate.

4. When the certificate is revoked, it is moved to the certificate revocation file.

5. The Public Key Certificate Revocation List is cut off at the end of each calendar year and records are retained 30 years from the date of cutoff. Records may be retained longer with customer consent or request.

6. Other records in this system are retained 7 years, unless retained longer by request of the customer.

7. Records related to electronic signatures are retained in an electronic database for 3 years.

8. Other categories of records are retained for a period of up to 30 days.

9. Driver's License data will be retained for 5 years.

10. COA and Hold Mail transactional data will be retained for 5 years.

11. Records related to Phone Verification/One-Time Passcode and Device Reputation assessment will be retained for 7 years.

12. Records collected for Identity Proofing at the Identity Assurance Level 2 (IAL-2), including ID document images, Identity Verification Attributes, and associated data will be retained up to 5 years, or as stipulated within Interagency Agreements (IAAs) with partnering Federal Agencies. Records existing on paper are destroyed by burning, pulping, or shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Access to these areas is limited to authorized personnel, who must be identified with a badge.

Access to records is limited to individuals who need the information to perform their job and whose official duties require such access.

Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections.

Computers are protected by mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software,

computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software.

Key pairs are protected against cryptanalysis by encrypting the private key and by using a shared secret algorithm to protect the encryption key, and the certificate authority key is stored in a separate, tamperproof, hardware device. Activities are audited, and archived information is protected from corruption, deletion, and modification.

For authentication services and electronic postmark, electronic data is transmitted via secure socket layer (SSL) encryption to a secured data center. Computer media are stored within a secured, locked room within the facility. Access to the database is limited to the system administrator, database administrator, and designated support personnel. Paper forms are stored within a secured area within locked cabinets.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES:

See Notification Procedure and Record Access Procedures above.

NOTIFICATION PROCEDURES:

Customers wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries must contain name, address, email, and other identifying information.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

March 16, 2020, 85 FR 14982; December 13, 2018, 83 FR 64164; December 22, 2017, 82 FR 60776; August 29, 2014, 79 FR 51627; October 24, 2011, 76 FR 65756; April 29, 2005, 70 FR 22516

Joshua J. Hofer,

Attorney, Ethics & Legal Compliance.

BILLING CODE P

[FR Doc. 2021-27113 Filed: 12/14/2021 8:45 am; Publication Date: 12/15/2021]